

# Generalized AG codes as evaluation codes

**Marco Calderini** (marco.calderini@unitn.it)

Department of Mathematics, University of Trento, Italy

**Massimiliano Sala** (maxsalacodes@gmail.com)

Department of Mathematics, University of Trento, Italy

---

## Abstract

We extend the construction of GAG codes to the case of evaluation codes. We estimate the minimum distance of these extended evaluation codes and we describe the connection to the one-point GAG codes.

**Keywords:** Evaluation codes, Affine-variety codes, AG codes, Generalized AG codes

---

## 1 Introduction

In 1999, Xing, Niederreiter and Lam proposed [NXL99,XNL99] two constructions of linear codes based on algebraic curves using points of arbitrary degree. These generalize the construction of Algebraic Geometry (AG) codes introduced by Goppa [Gop81,Gop82]. Özbudak and Stichtenoth [OS99] showed that there is essentially only one new construction, namely that of Generalized Algebraic Geometric (GAG) codes, and introduced the notion of designed minimum distance for GAG codes.

Until now several papers have studied GAG codes in an algebraic geometry way, see e.g. [Hey02], [DNX00], [CF12], [XY07].

Høholdt, van Lint and Pellikaan [HvLP98] founded the theory of order domains and of the order domain codes (or evaluation codes) to simplify the description of one-point AG codes. The minimum distance of evaluation codes can be found by applying bound that relies only on some relatively simple theory [HvLP98].

Affine-variety codes, introduced by Fitzgerald and Lax in [FL98], are particularly interesting for their parameters and for a new efficient decoding system [MOS12]. [Gei08] presents the AG codes as an example of affine-variety codes and their relation with evaluation codes.

In this paper we will extend the construction of affine-variety codes to introduce the GAG codes as a particular example of these family of codes.

We extend, also, the construction of the evaluation codes and we analyze a particular case of the one-point GAG codes into the setting of these new codes. The remainder of this paper contains the following sections.

- In Section 2 we recall definitions and theorems about the minimum distance for affine-variety codes, order domain codes and generalized algebraic geometric codes.
- In Section 3 we introduce two constructions of linear codes, the extended affine-variety codes and the extended order domain codes, and we estimate a lower bound on the minimum distance for these families of codes.
- In section 4 we analyze the relation between an extended order domain code and a GAG code constructed from a rational point and we compare the relevant bounds on the minimum distance of the code.

## 2 Preliminaries

### 2.1 Affine-variety codes

Let  $I \subseteq \mathbb{F}_q[X_1, \dots, X_m]$  be an ideal, we define

$$I_q = I + \langle X_1^q - X_1, \dots, X_m^q - X_m \rangle$$

$$R_q = \mathbb{F}_q[X_1, \dots, X_m]/I_q$$

Let

$$V = \{P_1, \dots, P_n\} = \mathcal{V}_{\mathbb{F}_q}(I) = \mathcal{V}_{\overline{\mathbb{F}_q}}(I_q)$$

be the variety of  $I$  over  $\mathbb{F}_q$ . Here  $\overline{\mathbb{F}}$  means the algebraic closure of the field  $\mathbb{F}$ .

Define the evaluation map  $ev : R_q \rightarrow \mathbb{F}_q^n$ , the  $\mathbb{F}_q$ -linear map such that

$$ev(f + I_q) = (f(P_1), \dots, f(P_n)). \quad (1)$$

The evaluation map is a vector space isomorphism.

**Definition 2.1.** *Let  $L$  be an  $\mathbb{F}_q$ -vector subspace of  $R_q$ . We define the affine variety code*

$$C(I, L) = ev(L).$$

The notation of this subsection comes from [FL98], where also the code  $C(I, L)^\perp$  is called an affine-variety code. In this paper we will not consider this type of codes.

### 2.2 Order domain conditions

Let  $J \subseteq \mathbb{F}[X_1, \dots, X_m]$  be an ideal and let  $\prec$  be a fixed monomial ordering. Denote by  $\mathcal{M}(X_1, \dots, X_m)$  the set of all monomials in the variables

$X_1, \dots, X_m$ . The footprint of  $J$  (or Hilbert staircase) with respect to  $\prec$  is the set

$$\Delta_{\prec}(J) = \{m \in \mathcal{M}(X_1, \dots, X_m) \mid m \text{ is not the leading monomial of any polynomial in } J\}.$$

**Definition 2.2.** Let  $I \subseteq \mathbb{F}[X_1, \dots, X_m]$  be an ideal. Let  $\prec_w$  be a generalized weighted degree ordering,  $w : \mathcal{M} \rightarrow \mathbb{N}_0^r$ . Assume  $I$  possesses a Gröbner basis  $\mathcal{G}$  such that:

- (i) any  $g \in \mathcal{G}$  has exactly two monomials of highest weight in its support.
- (ii) no two monomials in  $\Delta_{\prec_w}(I)$  are of the same weight.

Then we say that  $(I, \prec_w)$  satisfies the order domain conditions.

Let  $L \subseteq R_q$  be a subspace. By using Gaussian elimination any basis of  $L$  can be transformed into a basis of the following form.

**Definition 2.3.** Let  $\prec$  be a fixed monomial ordering and  $k = \dim(L)$ . A basis  $\{b_1 + I_q, \dots, b_k + I_q\}$  for  $L$  such that  $\text{Supp}(b_i) \subseteq \Delta_{\prec}(I_q)$  for  $i = 1, \dots, k$  and  $\text{lm}(b_1) \prec \dots \prec \text{lm}(b_k)$  is said to be well-behaving with respect to  $\prec$ . Here  $\text{lm}(f)$  means the leading monomial of  $f$ .

The sequence  $(\text{lm}(b_1), \dots, \text{lm}(b_k))$  is the same for all choices of well-behaving basis of  $L$ . So we define the set

$$\square_{\prec}(L) = \{\text{lm}(b_1), \dots, \text{lm}(b_k)\}.$$

**Definition 2.4.** Assume  $I$  and  $\prec_w$  satisfy the order domain conditions. Let  $\Gamma = w(\Delta_{\prec_w}(I)) \subseteq \mathbb{N}_0^r$  and  $\Delta = \Delta_{\prec_w}(I_q)$ . For any  $\lambda \in w(\Delta)$  we define

$$\sigma_{\Delta}(\lambda) = \sigma(\lambda) = |\{\eta \in w(\Delta) \mid \eta - \lambda \in \Gamma\}|.$$

**Theorem 2.5** (Th. 4.27 in [Gei08]). Assume  $(I, \prec_w)$  satisfies the order domain condition and let  $L$  subspace of  $R_q$  with  $\{b_1 + I_q, \dots, b_{\dim(L)} + I_q\}$  well-behaving basis. Then the minimum distance of  $C(I, L)$  is at least

$$\min\{\sigma(w(\alpha)) \mid \alpha \in \square_{\prec_w}(L)\}.$$

*Remark 2.6.* Assume that the pair  $(I, \prec_w)$  satisfies the order domain conditions. Let  $U \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$ . Every finite set of points is a variety and therefore there exists polynomials  $h_1, \dots, h_r$  such that the vanishing ideal of  $U$  equals

$$I_U = I + \langle h_1, \dots, h_r \rangle.$$

The estimates of the minimum distances of  $C(I, L)$  can be adapted if these codes are made by evaluating in  $U$  rather than in the entire variety, but we need to replace  $I_q$  with  $I_U$ .

### 2.3 Weight functions and order domains

The concept of a weight function was introduced by Høholdt et al. in [HvLP98] to simplify the treatment of one-point geometric AG codes and to propose a generalization to objects of higher dimensions than curves.

Let  $(R, \rho, \Gamma)$  be an order domain, where  $\Gamma \subseteq \mathbb{N}^r$  is a semigroup and  $\rho : R \rightarrow \Gamma \cup \{-\infty\}$  is a weight function.

From [GP02][Th. 10.4] we know that every order domain with a finitely generated semigroup,  $\Gamma$ , can be constructed as a factor ring,  $\mathbb{F}[X_1, \dots, X_m]/I$ . Therefore it can be described in the language of Gröbner basis theory.

**Definition 2.7.** Let  $R$  be an  $\mathbb{F}_q$ -algebra. A surjective map  $\phi : R \rightarrow \mathbb{F}_q^n$  is called a morphism of  $\mathbb{F}_q$ -algebras if  $\phi$  is  $\mathbb{F}_q$ -linear and if

$$\phi(fg) = \phi(f) * \phi(g)$$

for all  $f, g \in R$ . Here  $*$  is the component-wise product.

**Definition 2.8.** Let  $(R, \rho, \Gamma)$  be an order domain over  $\mathbb{F}_q$  and  $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$  be a basis. Let  $\phi : R \rightarrow \mathbb{F}_q^n$  be a morphism as in Definition 2.7. Define  $\alpha(1) = 0$ . For  $i = 2, \dots, n$  define recursively  $\alpha(i)$  to be the smallest element in  $\Gamma$  that is greater than  $\alpha(1), \dots, \alpha(i-1)$  and satisfies

$$\phi(f_{\alpha(i)}) \notin \text{Span}_{\mathbb{F}_q} \{\phi(f_\lambda) \mid \lambda \prec_{\mathbb{N}^r} \alpha(i)\}.$$

Write  $\Delta(R, \rho, \phi) = \{\alpha(1), \dots, \alpha(n)\}$ .

**Definition 2.9.** Let  $R$  be an order domain over  $\mathbb{F}_q$  and let  $\phi$  be a morphism. Fix a basis  $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$  and let  $\Delta = \Delta(R, \rho, \phi)$ . For  $\lambda \in \Gamma$  and  $\delta \in \mathbb{N}$  consider the codes

$$E(\lambda) = \text{Span}_{\mathbb{F}_q} \{\phi(f_\eta) \mid \eta \preceq_{\mathbb{N}^r} \lambda\}$$

$$\tilde{E}(\delta) = \text{Span}_{\mathbb{F}_q} \{\phi(f_\eta) \mid \eta \in \Delta \text{ and } \sigma_\Delta(\eta) \geq \delta\}.$$

**Theorem 2.10** (Th. 2 in [Gei09]). The minimum distance of  $E(\lambda)$  is at least

$$\min\{\sigma_\Delta(\eta) \mid \eta \preceq_{\mathbb{N}^r} \lambda\}$$

and the minimum distance of  $\tilde{E}(\delta)$  is at least  $\delta$ .

### 2.4 GAG codes

Let  $\mathcal{X}$  be a projective, geometrically irreducible, non-singular algebraic curve defined over the finite field  $\mathbb{F}_q$ . Let  $g$  be the genus of  $\mathcal{X}$ . Let  $\Phi$  be the Frobenius map on  $\mathcal{X}$ , namely the map sending a point  $P$  with homogeneous coordinates  $(a_0, \dots, a_r)$  to the point  $\Phi(P)$  with coordinates  $(a_0^q, \dots, a_r^q)$ .

Let  $P$  be a point of  $\mathcal{X}$ . Then  $\deg(P)$  denotes the degree of  $P$ , namely the least positive integer  $n$  such that  $P$  is  $\mathbb{F}_{q^n}$ -rational, and the closed point of  $P$  is the set  $O_\Phi(P) = \{P, \Phi(P), \dots, \Phi^{n-1}(P)\}$ .

Let  $\mathcal{X}$  be a curve, let  $P_1, \dots, P_s$  be points of  $\mathcal{X}$  such that for every  $i \neq j$  the closed points  $O_\Phi(P_i)$  and  $O_\Phi(P_j)$  are disjoint. Let  $G$  be an  $\mathbb{F}_q$ -rational divisor that has support disjoint from any closed point  $O_\Phi(P_i)$ . Let  $k_i := \deg(P_i)$ . For  $i = 1, \dots, s$  let  $\pi_i : \mathbb{F}_{q^{k_i}} \rightarrow C_i$  be an  $\mathbb{F}_q$ -linear isomorphism from the finite field  $\mathbb{F}_{q^{k_i}}$  onto a linear  $[n_i, k_i, d_i]$  code  $C_i \subseteq \mathbb{F}_q^{n_i}$ .

**Definition 2.11.** Let  $n = \sum_{i=1}^s n_i$ , and consider the  $\mathbb{F}_q$ -linear map

$$\pi : \begin{cases} \mathcal{L}(G) \rightarrow & \mathbb{F}_q^n \\ f \mapsto & (\pi_1(f(P_1)), \dots, \pi_s(f(P_s))) \end{cases}$$

The image of  $\pi$  is a Generalized Algebraic Geometric code

$$C(P_1, \dots, P_s; G; C_1, \dots, C_s) = \pi(\mathcal{L}(G)).$$

Here  $\mathcal{L}(G)$  denotes the Riemann-Roch space of  $G$  over  $\mathbb{F}_q$ .

The designed minimum distance  $\bar{d}$  of  $C(P_1, \dots, P_s; G; C_1, \dots, C_s)$  is defined as follows (see [OS99]): let

$$X = \left\{ S \subseteq \{1, \dots, s\} \mid \sum_{i \in S} k_i \leq \deg(G) \right\}.$$

Then

$$\bar{d} := \min \left\{ \sum_{i \notin S} d_i \mid S \in X \right\}$$

**Proposition 2.12** (Prop. 4.1 in [OS99]). If  $\sum_{i=1}^s k_i > \deg(G)$ , then  $C(P_1, \dots, P_s; G; C_1, \dots, C_s)$  is an  $[n, k, d]$  code with parameters

$$k = \dim(\mathcal{L}(G)) \geq \deg(G) + 1 - g \quad \text{and} \quad d \geq \bar{d}.$$

Throughout this paper, the codes  $C_i$  will be called the inner codes of the GAG code.

*Remark 2.13.* If we construct the GAG code using  $P_1, \dots, P_s$  points of which  $h$  are  $\mathbb{F}_q$ -rational, a divisor  $G$  with  $\deg(G) \leq h$  and inner codes having minimum distance all equals to 1, then the designed minimum distance is equal to  $s - \deg(G)$ .

### 3 New construction of codes

For any  $v \in \mathbb{F}_q^n$ , let  $w_H(v) = |\{i \mid v_i \neq 0\}|$ .

### 3.1 Extended Affine-variety codes

Let  $(I, \prec_w)$  satisfying the order domain condition and let  $\mathcal{P} = \{P_1, \dots, P_h\} \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$ , with  $\deg(P_i) = r_i$  for  $i = 1, \dots, h$ . As in Remark 2.6 there is an ideal  $J \subseteq \mathbb{F}_q[X_1, \dots, X_m]$  such that  $\mathcal{P} = \mathcal{V}_{\mathbb{F}_q}(I + J)$ . Let  $I + J = I_{\mathcal{P}}$ .

Let  $L$  be a space over  $\mathbb{F}_q$  with well-behaving basis  $B = \{b_1 + I_{\mathcal{P}}, \dots, b_k + I_{\mathcal{P}}\}$ , and for  $i = 1, \dots, h$  let  $\pi_i : \mathbb{F}_{q^{r_i}} \rightarrow C_i$  be an  $\mathbb{F}_q$ -linear isomorphism from the finite field  $\mathbb{F}_{q^{r_i}}$  onto the inner code  $C_i$  over  $\mathbb{F}_q$  with parameters  $[n_i, r_i, d_i]$ .

**Definition 3.1.** Let  $n = \sum_{i=1}^h n_i$ ,  $\mathcal{P} = \{P_1, \dots, P_h\}$  and  $\mathcal{C} = \{C_1, \dots, C_h\}$ . Consider the  $\mathbb{F}_q$ -linear map,

$$\overline{ev} : \begin{cases} L \rightarrow \mathbb{F}_q^n \\ f \mapsto (\pi_1(f(P_1)), \dots, \pi_h(f(P_h))) \end{cases}$$

Then the extended affine-variety code is

$$\overline{ev}(L) = C(I, L, \mathcal{P}, \mathcal{C}).$$

**Theorem 3.2.** Let  $\Delta = \Delta_{\prec_w}(I_{\mathcal{P}})$ , then  $C(I, L, \mathcal{P}, \mathcal{C})$  has minimum distance at least

$$\delta \hat{d},$$

where  $\delta = \min\{\sigma(w(\alpha) \mid \alpha \in \square(L)\}$  and  $\hat{d} = \min\{d_1, \dots, d_h\}$ .

*Proof.* Let  $r = m.c.m.\{r_1, \dots, r_h\}$  and  $B$  be a well-behaving basis for  $L$ . Consider

$$L' = \text{Span}_{\mathbb{F}_{q^r}} B$$

and let  $ev(L') \subseteq (\mathbb{F}_{q^r})^h$  (where  $ev$  is as in (1)) be the affine variety code over  $\mathbb{F}_{q^r}$  restricted at the points  $P_1, \dots, P_h$ . From Theorem 2.5, the minimum distance of this code is at least  $\delta$ .

Note that  $L \subseteq L'$ , then for every non zero  $c \in ev(L)$  we have  $w_H(c) \geq \delta$ .

Let  $\bar{c} \in C(I, L, \mathcal{P}, \mathcal{C}) \setminus \{0\}$ , then  $\bar{c} = (\pi_1(f(P_1)), \dots, \pi_h(f(P_h)))$  for some  $f$ . So let  $S = \{i \mid f(P_i) \neq 0\}$ , we have

$$w_H(c) = \sum_{i=1}^r w_H(\pi_i(f(P_i))) = \sum_{i \in S} d_i \geq \delta \hat{d}.$$

□

*Remark 3.3.* We can estimate the minimum distance of the extended code  $C(I, L, \mathcal{P}, \mathcal{C})$  also if the order domain conditions are not satisfy. We can look at the number of one-way well-behaving pairs (see Def. 4.8 in [Gei08]) as in Th. 4.9 in [Gei08]. So we are able to obtain a bound similar to Theorem 3.2.

### 3.2 Extended Order Domain codes

Let  $(R, \rho, \Gamma)$  be an order domain over  $\mathbb{F}_q$  and  $B$  be a well-behaving basis for  $R$ . Consider  $R' = \text{Span}_{\mathbb{F}_{q^r}} B$ , then  $(R', \rho, \Gamma)$  is an order domain over  $\mathbb{F}_{q^r}$ . Note that  $R \subseteq R'$ .

Now let  $\phi : R' \rightarrow \mathbb{F}_{q^r}^h$  be a morphism  $\phi = (\phi_1, \dots, \phi_h)$ . For  $i = 1, \dots, h$  define  $r_i = \min\{l \mid \phi_i(R) \subseteq \mathbb{F}_{q^l}\}$ .

Let  $\Delta = \Delta(R', \rho, \Gamma)$  be as in Definition 2.8. For  $i = 1, \dots, h$  let  $\pi_i : \mathbb{F}_{q^{r_i}} \rightarrow C_i$  be an  $\mathbb{F}_q$ -linear isomorphism from the finite field  $\mathbb{F}_{q^{r_i}}$  onto the inner code  $C_i$  over  $\mathbb{F}_q$  with parameters  $[n_i, r_i, d_i]$ .

**Definition 3.4.** Let  $\mathcal{C} = \{C_1, \dots, C_h\}$  and  $\mathcal{R} = \{r_1, \dots, r_h\}$ . For  $\lambda \in \Gamma$  and  $\delta \in \mathbb{N}$  consider the codes

$$E(\lambda, \mathcal{R}, \mathcal{C}) = \text{Span}_{\mathbb{F}_q} \{(\pi_1(\phi_1(f_\eta)), \dots, \pi_h(\phi_h(f_\eta))) \mid \eta \preceq_{\mathbb{N}^r} \lambda\}$$

$$\hat{E}(\delta, \mathcal{R}, \mathcal{C}) = \text{Span}_{\mathbb{F}_q} \{(\pi_1(\phi_1(f_\eta)), \dots, \pi_h(\phi_h(f_\eta))) \mid \eta \in \Delta \text{ and } \sigma_\Delta(\eta) \geq \delta\}.$$

**Theorem 3.5.** The minimum distance of  $E(\lambda, \mathcal{R}, \mathcal{C})$  is at least

$$\gamma \hat{d},$$

where  $\gamma = \min\{\sigma_\Delta(\eta) \mid \eta \preceq_{\mathbb{N}^r} \lambda\}$  and  $\hat{d} = \min\{d_1, \dots, d_h\}$ .

The minimum distance of  $\hat{E}(\delta, \mathcal{R}, \mathcal{C})$  is at least  $\delta \hat{d}$ .

*Proof.* Obvious adaption of the proof at Theorem 3.2.  $\square$

## 4 One-point GAG codes as Extended Order Domain codes

Now we consider the GAG codes constructed from a rational point of the curve, using as inner code  $C_i = \mathbb{F}_q^{r_i}$  for  $i = 1, \dots, h$ . We refer to these as one-point GAG codes.

Let  $P$  be a rational point of a curve  $\mathcal{X}$  defined over a field  $\mathbb{F}_q$ . Let  $\nu_P$  be the valuation corresponding to  $P$ . Consider the algebraic structure

$$R = \bigcup_{m=0}^{\infty} \mathcal{L}(mP). \quad (2)$$

Defining  $\rho = -\nu_P$  we have  $\rho(R) = \Gamma \cup \{-\infty\}$  where  $\Gamma \subseteq \mathbb{N}$  is known as the Weierstrass semigroup corresponding to  $P$ . By inspection  $(R, \rho, \Gamma)$  is an order domain over  $\mathbb{F}_q$ .

Let  $P_1, \dots, P_h$  be distinct points, with distinct closed points, of degree  $r_1, \dots, r_h$ , respectively. Let  $B$  be a well-behaving basis for  $R$ . Define  $R' = \text{Span}_{\mathbb{F}_{q^r}} B$  and let  $\phi : R' \rightarrow \mathbb{F}_{q^r}^h$  be a morphism with  $\phi(f) = (f(P_1), \dots, f(P_h))$ .

Then we have

$$C(P_1, \dots, P_h, \lambda P, C_1, \dots, C_h) = C(I, L, \mathcal{P}, \mathcal{C}) = E(\lambda, \mathcal{R}, \mathcal{C}),$$

where  $L = \{f \mid \rho(f) \leq \lambda\}$ ,  $\mathcal{P} = \{P_1, \dots, P_h\}$ ,  $\mathcal{R} = \{r_1, \dots, r_h\}$  and  $\mathcal{C} = \{C_1, \dots, C_h\}$ .

**Lemma 4.1** (Lemma 2 in [Gei09]). *Let  $\Gamma = \{\lambda_1, \lambda_2, \dots\}$  with  $\lambda_1 < \lambda_2 < \dots$  be a numerical semigroup with finitely many gaps. For any  $\lambda_i$  we have*

$$\#(\Gamma \setminus (\lambda_i + \Gamma)) = \lambda_i.$$

**Theorem 4.2.** *The minimum distance of  $E(\lambda, \mathcal{R}, \mathcal{C})$  is at least*

$$\min\{\sigma_\Delta(\eta) \mid \eta \leq \lambda\} \geq h - \lambda$$

where  $\Delta = \Delta(R', \rho, \phi)$ .

*Proof.* The distances of the inner codes are all equal to 1. Consider  $\lambda_i \in \Delta$ , with  $\lambda_i \leq \lambda$ . We have  $\sigma(\lambda_i) = \#(\Delta \cap (\lambda_i + \Gamma))$ , the elements in  $\Delta$  that are not in  $\lambda_i + \Gamma$  are at most  $\lambda_i$ . Then  $\sigma(\lambda_i) \geq h - \lambda_i \geq h - \lambda$ .  $\square$

*Remark 4.3.* With order domain code it is possible, sometimes, to have a bound on the minimum distance of a one-point Algebraic Geometry code better than the Goppa bound [Gei09]. So also for GAG codes, if we are in the case as in the Remark 2.13, using the order domains is possible to obtain a bound always at least as good as (and sometimes better than) the bound in the Proposition 2.12.

**Example 4.4.** Let  $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ , where  $\alpha$  is a primitive element. Consider the plane curve of affine equation  $\mathcal{X} : X^6 + Y^5 + Y$ . Let  $\prec$  be the weighted degree lexicographic ordering given by  $w(X) = 5, w(Y) = 6$ . Let  $I = \langle X^6 + Y^5 + Y \rangle$ , then  $(I, \prec)$  satisfies the order domain conditions and  $w(\Delta(I))$  is the semigroup  $\langle 5, 6 \rangle$ .

We have 8  $\mathbb{F}_4$ -rational points

$$\mathcal{V}(I_4) = \{(0, 0), (0, 1), (1, \alpha), (1, \alpha^2), (\alpha, \alpha), (\alpha, \alpha^2), (\alpha^2, \alpha), (\alpha^2, \alpha^2)\}$$

and  $\mathcal{G} = \{Y^2 + X^3 + Y, XY^2 + XY + X, Y^4 + Y\}$  is a Gröbner basis for  $I_4$ . The monomials in the footprint of  $I_4$  are

$$\Delta(I_4) = \{1, X, Y, X^2, XY, Y^2, X^2Y, Y^3\}$$

and its corresponding weights are

$$w(\Delta(I_4)) = \{0, 5, 6, 10, 11, 12, 16, 18\}.$$

Now we consider a point of the variety  $\mathcal{V}_{\mathbb{F}_4}(I)$  of degree 3 (there are not points of degree 2). Let  $\mathbb{F}_{64} = \mathbb{F}_4[Z]/\langle Z^3 + Z + 1 \rangle$  and let  $\beta^3 = \beta + 1$ . The



point that we consider is  $(1, \beta^3)$ . Using Buchberger-Möller's algorithm we can compute the Gröbner basis of the vanishing ideal of the nine points, so we adjoin the monomial  $X^3$  at the footprint and the weight 15 to  $w(\Delta(I_4))$ .

Consider now  $L = \text{Span}_{\mathbb{F}_4}\{1, X, Y\}$ , then the minimum distance of  $C(I, L, \mathcal{P}, \mathcal{C})$ , where the inner code used are  $C_1 = \dots = C_8 = \mathbb{F}_4$  and  $C_9 = \mathbb{F}_4^3$ , is at least  $\min\{\sigma(0), \sigma(5), \sigma(6)\} = 5$ . This value improves on what obtainable from the GAG construction, as follows.

Looking at this code as a one-point GAG code we can note that the semigroup  $w(\Delta(I))$  is the Weierstrass semigroup of the unique rational point at infinity,  $P_\infty$ , of the curve and  $L = \mathcal{L}(6P_\infty)$ . Therefore the bound on minimum distance of the GAG code as in Proposition 2.12 is equal to 3.

In [Mat99] was shown that an order domain with numerical weight function (i.e. the weights are in  $\mathbb{N}_0$ ) is a sub algebra of a structure as in (2). If the semigroup related to the order domain are not numerical then they are related to structures of transcendence degree greater than one, that is, these structures are curves no longer ([GP02] Sec. 11). Examples of evaluation codes coming from higher dimensional objects than curves are given in [AG08] and these codes can be viewed as generalizations of one-point AG codes. Then our extension can be consider a generalization of the one-point GAG codes.

## References

- [AG08] H. E. Andersen and O. Geil, *Evaluation codes from order domain theory*, Finite Fields Appl. **14** (2008), 92–123.
- [CF12] M. Calderini and G. Faina, *Generalized algebraic geometric codes from maximal curves*, IEEE Transactions on Information Theory **58** (2012), no. 4, 2386–2396.
- [DNX00] C. Ding, H. Niederreiter, and C. Xing, *Some new codes from algebraic curves*, Information Theory, IEEE Transactions on **46** (2000), no. 7, 2638–2642.
- [FL98] J. Fitzgerald and R. F. Lax, *Decoding affine variety codes using Gröbner bases*, Des. Codes Cryptogr. **13** (1998), no. 2, 147–158.
- [Gei08] O. Geil, *Evaluation codes from an affine variety code perspective*, ALGEBRAIC GEOMETRY CODES (2008), 153.
- [Gei09] ———, *Algebraic geometry codes from order domains*, Gröbner Bases, Coding, and Cryptography (2009), 121–141.
- [Gop81] V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. **24** (1981), no. 1, 170–172.
- [Gop82] V.D. Goppa, *Algebraico-geometric codes*, Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya **46** (1982), no. 4, 762–781.

- [GP02] O. Geil and R. Pellikaan, *On the structure of order domains*, Finite Fields and their Applications **8** (2002), no. 3, 369–396.
  - [Hey02] A.E. Heydtmann, *Generalized geometric goppa codes*, Communications in Algebra **30** (2002), no. 6, 2763–2789.
  - [HvLP98] T. Høholdt, J. H. van Lint, and R. Pellikaan, *Algebraic geometry of codes*, Handbook of coding theory, Vol. I, II (V. S. Pless and W.C. Huffman, eds.), North-Holland, 1998, pp. 871–961.
  - [Mat99] R. Matsumoto, *Miura’s generalization of one-point AG codes is equivalent to Høholdt, van Lint and Pellikaan’s generalization*, IEICE Trans. Fund. **E82-A** (1999), no. 10, 2007–2010.
  - [MOS12] C. Marcolla, E. Orsini, and M. Sala, *Improved decoding of affine-variety codes*, Journal of Pure and Applied Algebra **216** (2012), no. 7, 1533–1565.
  - [NXL99] H. Niederreiter, C. Xing, and K.Y. Lam, *New construction of algebraic-geometry codes*, APPL ALGEBRA ENG COMMUN COMPUT **9** (1999), no. 5, 373–381.
  - [OS99] F. Ozbudak and H. Stichtenoth, *Constructing codes from algebraic curves*, Information Theory, IEEE Transactions on **45** (1999), no. 7, 2502–2505.
  - [XNL99] C. Xing, H. Niederreiter, and K.Y. Lam, *A generalization of algebraic-geometry codes*, Information Theory, IEEE Transactions on **45** (1999), no. 7, 2498–2501.
  - [XY07] C. Xing and S.L. Yeo, *New linear codes and algebraic function fields over finite fields*, Information Theory, IEEE Transactions on **53** (2007), no. 12, 4822–4825.
-